

**THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY  
OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:**

1. A method of generating a key by a first correspondent, wherein said key is computable by a  
5 second correspondent, said method comprising the steps of:

- a) making available to said second correspondent a first short term public key;
- b) obtaining a second short term public key from said second correspondent;
- c) computing a first exponent derived from said first short term private key, said first short  
term public key, and said first long term private key;
- 10 d) computing a second exponent derived from said first short term private key, said first  
long term public key, said second short term public key and said first long term private  
key;

computing a simultaneous exponentiation of said first exponent with said second short term  
public key and said second exponent with said second long term public key.